TCP/IP に係る既知の脆弱性検証ツールの開発

株式会社ラック　磯 貴浩、直岡 克起、吉永 昇

概要

TCP/IP に係る既知の脆弱性が多数公表されている。これらの脆弱性の中には、脆弱性と言えるのかどうか曖昧なものや、仕様上の問題で、対策が難しいものも含まれている。新しい TCP/IP の実装を作り込む場合には、このような既知の脆弱性を十分考慮する必要がある。また、新しい TCP/IP の実装に対して、これらの既知の脆弱性が存在しないかを検証するツールが必要である。

本プロジェクトでは、TCP/IP に係る既知の脆弱性についての情報を、調査報告書としてまとめ、それらの脆弱性の有無を検証するツールを開発した。

1. 背景

コンピュータ、機器に広く組み込まれている TCP/IP ソフトウェアに関し多数の脆弱性が公表されているが、このような既に知られている脆弱性であっても、新たに開発されたソフトウェアにおいて、対策がとられていない場合がある。これらの脆弱性は、内容を理解する為に高度な技術力が必要とされるものが多いが、日本語による詳細な情報がまとめられていないのが現状である。

また、新たに開発したソフトウェアが、これらの脆弱性を持っているか否かを容易に確認する手段がないことも問題である。

TCP/IP ソフトウェアに関する脆弱性について調査を行い、日本語による詳細な情報をまとめ、さらに、それらの脆弱性の有無を簡単に確認するツールを開発することによって、これらの脆弱性を含んだまま新しく世に送り出されるソフトウェアを減少させる。あるいは、TCP/IP ソフトウェアに関する脆弱性への取り組みを活性化させることが期待されている。

2. 目的

既に知られている TCP/IP ソフトウェアの脆弱性を調査し、詳細な情報を報告書の形でまとめる。また、これらの脆弱性が、新たに開発されたソフトウェアに存在するか否かを確認するツールを開発する。

これらの報告書とツールを、TCP/IP ソフトウェアに係る製品開発者に提供し、広範囲に影響のある TCP/IP ソフトウェア製品の脆弱性を低減することを、本プロジェクトの目的とする。

3.　概要

本プロジェクトには、調査作業と開発作業が含まれる。

調査作業においては、既に知られているTCP/IP ソフトウェアの脆弱性を、一般に公表されている資料から調査し、報告書に取り纏める。

開発作業においては、ソフトウェア開発者（以降、利用者）向けの TCP/IP ソフトウェア脆弱性検証ツール、確認ツールを開発する。調査作業の中で、このツールに組み込むべき脆弱性項目を選択し、利用者が新しく開発したソフトウェアに選択した脆弱性項目が存在するか否かを判定するツールである。

利用者は、検証ツール、確認ツールを使用して、TCP/IP に係わる脆弱性が新しく開発したソフトウェアに存在するか否かを調査し、報告書を参照して脆弱性の意味や対策方法を知ることができる。

図 1、図 2 にこのプロジェクトの成果物である脆弱性検証ツールと、脆弱性報告書の利用イメージを示す。

利用者は、インストール CD から脆弱性検証ツール動作 PC に脆弱性検証ツールのプログラムをインストールし、GUI を操作することによって検証対象機器に脆弱性が存在するか否かを調査する。調査結果の詳細な内容は、脆弱性報告書を参照して知ることができる。(図 1)

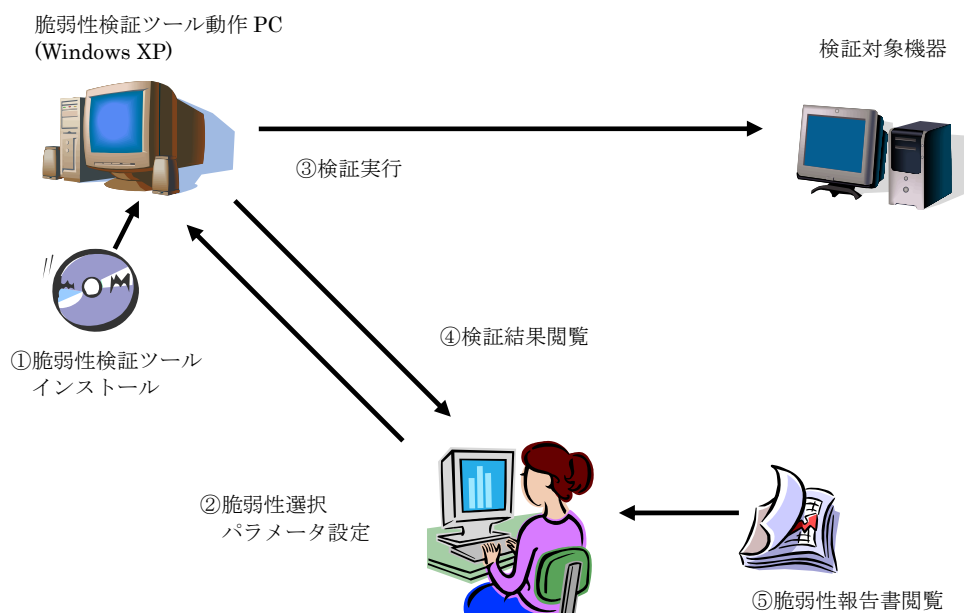



図 1

また、インストールCDから脆弱性確認ツール動作 PC に脆弱性確認ツールのプログラムをインストールし、GUI を操作することによって脆弱性検証ツールが送信したパケットが検証対象機器を通過した否かを確認することにより、検証対象機器に脆弱性が存在するか否かを調査する。(図 2)

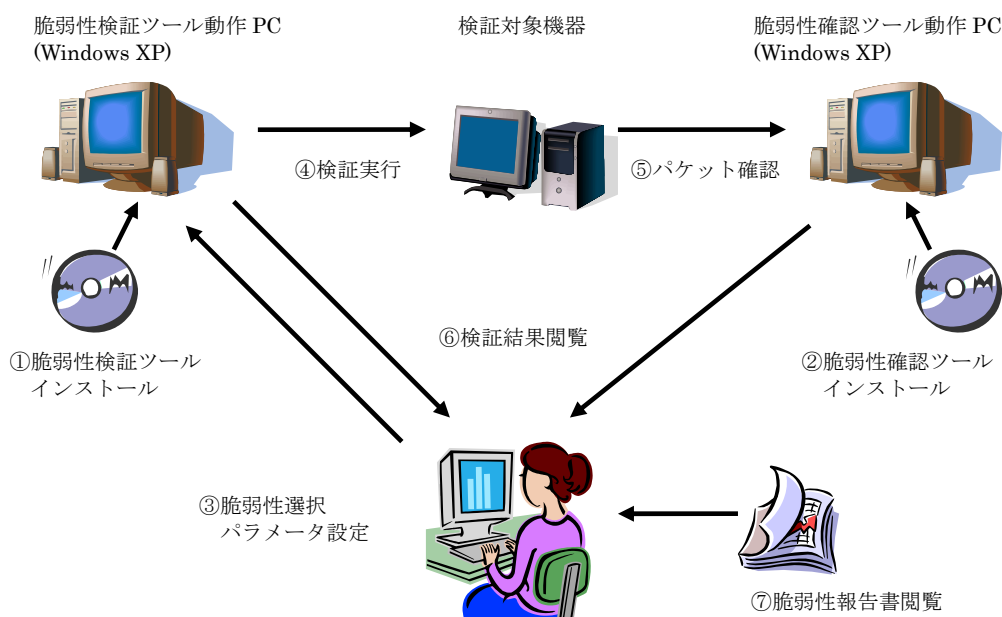



図 2

4. 調査報告書

(1) 全体像

TCP/IP に係る既知の脆弱性について、文献、Web、弊社既存資料を用いて情報収集を行い、内容の検証し、考察を加えて調査報告書にまとめた。攻撃手法、原因の説明には豊富な図を用いた。また、発見の経緯とトピック、対策の動き、現在の動向、IPv6 環境における影響を記載した。対策方法については、実装に関する部分と、運用に関する部分に分け、実装ガイド、運用ガイドという項目にまとめた。

(2) 調査対象

調査対象として、以下の 23 項目を選定した。

表 1

No	項目名
1	TCP の初期シーケンス番号予測 の問題
2	TCP 接続の強制切断 の問題
3	SYN パケットにサーバ資源が占有される問題 (SYN Flood Attack)
4	特別な SYN パケットによりカーネルがハングアップする問題 (LAND Attack)
5	データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題(Overlapping Fragment Attack)

6	十分に小さい分割パケットがフィルタリングをすり抜ける問題(Tiny Fragment Attack, Tiny Overlapping Fragment Attack)
7	PAWS 機能の内部タイマを不正に更新することで、TCP 通信が強制的に切断される問題
8	Optimistic TCP acknowledgements により、サービス不能状態に陥る問題
9	Out of Band(OOB)パケットにより、サービス不能状態に陥る問題
10	パケット再構築時にバッファが溢れる問題(Ping of death)
11	ICMP Path MTU Discovery 機能を利用した通信遅延の問題
12	ICMP リダイレクトによるサービス応答遅延の問題
13	ICMP リダイレクトによる送信元詐称の問題
14	ICMP 始点制御メッセージによる通信遅延の問題
15	ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題(ICMP トンネリング)
16	ICMP エラーにより TCP 接続が切断される問題
17	ICMP Echo リクエストによる帯域枯渇の問題(Ping flooding, Smurf Attack, Fraggle Attack)
18	フラグメントパケットの再構築時にシステムがクラッシュする問題(Teardrop Attack)
19	パケット再構築によりメモリ資源が枯渇される問題(Rose Attack)
20	IP 経路制御オプションが検査されていない問題
21	ARP テーブルが汚染される問題
22	ARP テーブルが不正なエントリで埋め尽くされる問題
23	通常でないパケットへの応答によって OS の種類が特定できる問題(TCP/IP Stack Fingerprinting)

5. ソフトウェア

(1) システム構成

本プロジェクトで開発したソフトウェアは、TCP/IP ソフトウェア脆弱性検証ツール、確認ツールの 2 つである。Windows XP Professional を搭載した IBM AT 互換機上で動作する。それぞれのツールは、各種指示を行うメインプログラムと、攻撃パケットを送信/受信する脆弱性検証モジュールの２つに分かれる。

(2) 機能

● 攻撃シミュレーション機能

表 2 に示す 18 の脆弱性検証モジュールを有する(IPv6 に関しては 2 つの脆弱性検証モジュール)。

このモジュールは、当該脆弱性を突く攻撃パケットを送信する機能を持つ。

脆弱性検証モジュールは、今後、追加することが可能である。

表 2

No	IPv4	IPv6	項目名
1	○	―	TCP の初期シーケンス番号予測の問題
2	○	○	SYN パケットにサーバ資源が占有される問題 (SYN Flood Attack)
3	○	―	特別な SYN パケットによりカーネルがハングアップする問題(LAND Attack)
4	○	○	データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題 (Overlapping Fragment Attack)
5	○	―	十分に小さい分割パケットがフィルタリングをすり抜ける問題(Tiny Fragment Attack, Tiny Overlapping Fragment Attack)
6	○	―	Out of Band(OOB)パケットにより、サービス不能状態に陥る問題
7	○	―	パケット再構築時にバッファが溢れる問題(Ping of death)
8	○	―	ICMP Path MTU Discovery 機能を利用した通信遅延の問題
9	○	―	ICMP リダイレクトによるサービス応答遅延の問題
10	○	―	ICMP リダイレクトによる送信元詐称の問題
11	○	―	ICMP 始点制御メッセージによる通信遅延の問題
12	○	―	ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題(ICMP トンネリング)
13	○	―	ICMP エラーにより TCP 接続が切断される問題
14	○	―	ICMP Echo リクエストによる帯域枯渇の問題(Ping flooding, Smurf Attack, Fraggle Attack)
15	○	―	フラグメントパケットの再構築時にシステムがクラッシュする問題(Teardrop Attack)
16	○	―	パケット再構築によりメモリ資源が枯渇される問題(Rose Attack)
17	○	―	ARP テーブルが汚染される問題
18	○	―	ARP テーブルが不正なエントリで埋め尽くされる問題

○：実装

－：未実装

● サービス監視機能

検証対象の機器に対して、任意の TCP ポートが接続可能かどうかを、検証中と検証終了後に定期的に監視し、脆弱性に対する効果の有無を調査することができる。接続不能な状態が指定した回数連続して発生すると、効果が有ったと判定する。ただし、脆弱性に対する効果の有無は、この機能だけでは判断することはできない。判断に対する１つの材料として活用できる。

脆弱性に対する効果の確認方法については、取扱説明書に詳しく明記している。

(3) ユーザインターフェイス(検証ツール)

● 脆弱性項目の選択

図 3 に、脆弱性項目の選択画面を示す。

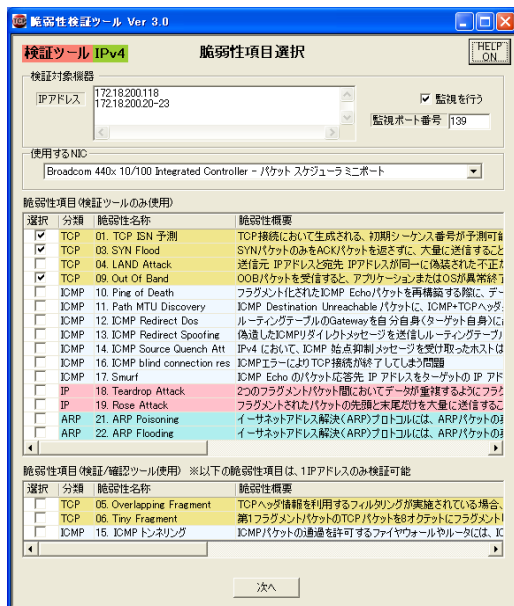



図 3

以下の項目を設定する。

- 検証対象機器の IP アドレス、
- サービス監視機能の監視ポート番号
- 仕様する NIC の選択

- 脆弱性項目の選択

［次へ］ボタンをクリックすると、選択された脆弱性項目のパラメータ設定画面が順次表示される。

● パラメータの設定

図 4 にパラメータ設定画面を示す。

図 4

脆弱性項目毎に、攻撃パケットに関するパラメータとサービス監視に関するパラメータを入力する。これらのパラメータの設定方法については、取扱説明書にて詳しく解説している。

● 脆弱性検証実行

図 5 に、脆弱性検証実行画面を示す。

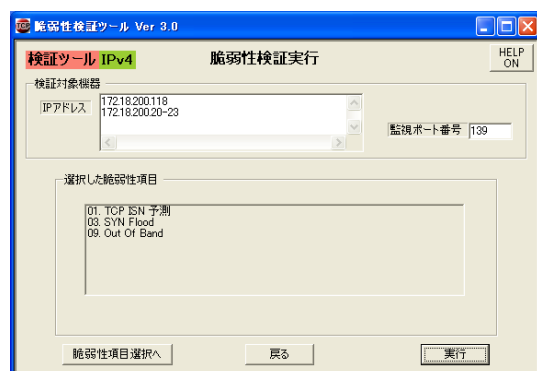



図 5

選択した脆弱性項目が表示される。ここで［実行］ボタンをクリックすると、検証を

開始する。

● 脆弱性検証確認

図 6 に、脆弱性検証確認画面を示す。

図 6

検証状況と脆弱性判定が表示される。

検証状況では、表 3 に示す表示が行われる。

表 3

表示内容	説明
―	まだ実行されていません
検証中	検証を行っています
監視中	サービスの監視を行っています
エラー	攻撃パケットの送信処理において、エラーが発生しました ネットワークの接続を確認してください また、送信間隔とパケット送信回数を調整して、再度検証を行ってください
完了	検証と監視が終了しました

脆弱性判定では、表 4 に示す表示が行われる。

脆弱性判定は、単純なサービスポートの監視結果を見ているに過ぎない。実際の脆弱性の有無は、検証対象機器の状態を、検証者が確認する必要がある。確認方法については、取扱説明書にて詳しく解説している。

表 4

表示内容	説明
―	まだ判定されていません あるいは、サービス監視を行いませんでした あるいは、検証がエラーとなりました
無し	サービス監視で異常はありませんでした
有り	サービス監視で異常の回数がしきい値に達しました
有りの疑い	サービス監視で異常がありましたが、回数がしきい値に達しませんでした

(4) ユーザインターフェイス(確認ツール)

● 脆弱性項目の選択

図 7 に、脆弱性項目の選択画面を示す。

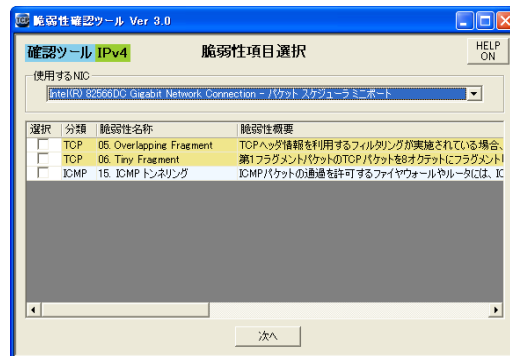



図 7

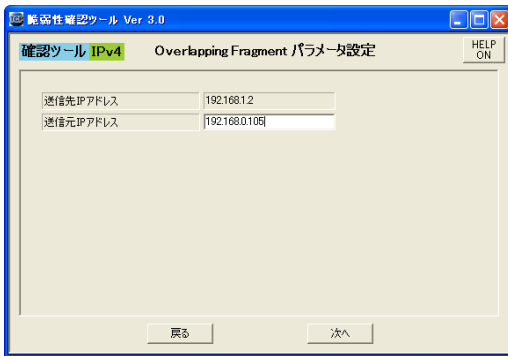
以下の項目を設定する。

- 仕様する NIC の選択
- 脆弱性項目の選択

［次へ］ボタンをクリックすると、選択された脆弱性項目のパラメータ設定画面が順次表示される。

● パラメータの設定

図 8 にパラメータ設定画面を示す。

図 8

脆弱性項目毎に、攻撃パケットに関するパラメータを入力する。これらのパラメータの設定方法については、取扱説明書にて詳しく解説している。

- 脆弱性検証実行

図 9 に、脆弱性検証実行画面を示す。

図 9

選択した脆弱性項目が表示される。ここで[実行]ボタンをクリックすると、検証を開始する。

- 脆弱性検証確認

図 10 に、脆弱性検証確認画面を示す。

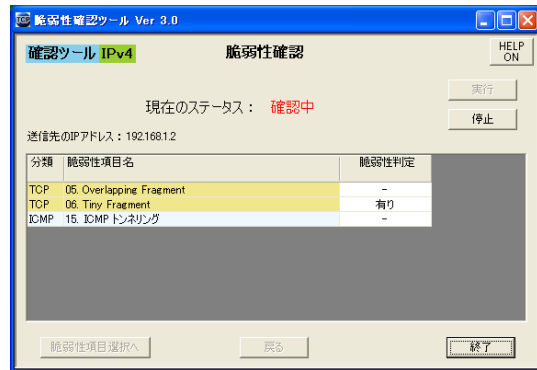



図 10

脆弱性判定では、表 5 に示す表示が行われる。

脆弱性判定は、検証ツールから送信されたパケットを受信すると検証対象機器に脆弱性ありと判断し”有り”と表示される。

表 5

表示内容	説明
－	まだ判定されていません あるいは、確認処理がエラーとなりました
有り	検証ツールから送信された脆弱性のパケットを受信しました。

6. まとめ

この検証ツールは、インターネットに接続する機器に組込むソフトウェア、特に、TCP/IP の新しい実装に対して検証を行うことを目的として開発した。

今回、検証ツールで開発した脆弱性項目は IPv4 に関して 18 項目、IPv6 に関して 2 項目である。この項目は追加することが可能であり、特に IPv6 に関しては、今後の普及状況により、計画的な追加開発が必要と考えている。

7. 謝辞

この調査・開発には、次の方々にもご協力いただきました。この場を借りて、御礼申し上げます。

- 株式会社インターネットイニシアティブ（IIJ）
- 有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）
- 日本電気株式会社
- パナソニックコミュニケーションズ株式会社
- 株式会社 日立製作所
- 富士通株式会社
- 松下電器産業株式会社
- ヤマハ株式会社

－ 以上 －